УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА
Том 153, кн. 4 Физико-математические науки *2011*

УДК 621.396.969.1+621.391.7

МОДЕЛИРОВАНИЕ СИНХРОННОЙ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ В МЕТЕОРНОМ РАДИОКАНАЛЕ

А.И. Сулимов, А.В. Карпов, О.Н. Шерстюков, В.В. Сидоров, Р.Г. Хузяшев

Аннотация

В работе производится оценка битовой скорости генерации ключа симметричного шифрования из общего для двух пунктов связи источника природной случайности, в качестве которого используется метеорный радиоканал. Рассмотрена общая методика генерации ключевой последовательности на основе физических свойств метеорного радиоканала и методика оценки ее средней скорости. Рассмотрены основные аппаратурные и физические факторы, ограничивающие ее величину. На основе строгого решения задачи дифракции радиоволн на метеорном следе исследованы основные закономерности фазовой невзаимности на метеорных радиолиниях различной длины, рассмотрены причины ее возникновения и даны количественные оценки.

Ключевые слова: ключ симметричного шифрования, распределение криптографических ключей, метеорный радиоканал, дифракция радиоволн, невзаимность, нестабильность, имитационная модель, энтропия, скорость передачи данных.

Введение

Проблема распределения ключей шифрования в симметричных криптосистемах является одной из фундаментальных проблем криптографии [1]. Согласно теореме Шеннона о совершенных криптосистемах [2] теоретическую нераскрываемость шифра возможно достичь при соблюдении двух условий: 1) каждое секретное сообщение должно шифроваться с использованием уникального ключа, 2) объем секретного сообщения не должен превосходить объема ключа шифрования. Длительное время выполнение указанных условий представлялось технически неосуществимым. В работах [3–5] был предложен оригинальный способ генерации и дистанционного распределения криптографических ключей на расстояние до 2000 км, основанный на физических свойствах метеорного распространения радиоволн – «метеорная криптография». На сегодняшний день это единственный известный способ безопасной передачи ключей на столь большие расстояния. Однако его эффективность до сих пор систематически не исследована, не произведены оценки влияния невзаимности и нестабильности метеорного распространения радиоволн.

Целью настоящей статьи является построение имитационной модели системы метеорной криптографии для оценки ее производительности.

1. Методика генерации ключевой последовательности

Процесс формирования ключевой последовательности на основе стохастических свойств метеорного радиоканала (МРК) может быть проиллюстрирован с помощью блок-схемы на рис. 1. Ввиду непредсказуемости возникновения метеорных следов

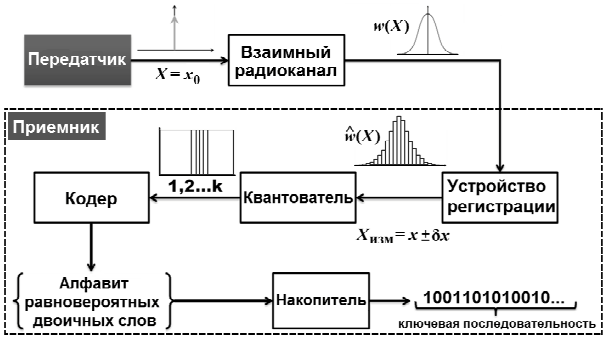


Рис. 1. Блок-схема формирования ключевой последовательности

во времени и пространстве траектория метеорного распространения сигнала является случайной. Фаза и время распространения сигнала при этом также будут случайными величинами. Кроме того, ряд экспериментальных исследований свидетельствует о достаточной для технических приложений взаимности метеорного радиоканала [6–8]. Теоретически это означает, что, обмениваясь встречными сигналами и накапливая на обеих сторонах радиолинии наборы измерений их фазы или времени распространения, стороны могут сформировать идентичные наборы случайных чисел. В [9] предложено использовать такие наборы для создания двух экземпляров единого ключа симметричного шифрования. Реализация этого способа требует сверхточной синхронизации пунктов связи. В [8] экспериментально доказано, что метеорные системы синхронизации способны обеспечить погрешность синхронизации $\delta\tau_c$ менее 1 нс, что вполне достаточно для реализации метеорной криптографии.

В общем случае МРК не является взаимным, что вызывает различия регистрируемых в пунктах A и B измерений фазы и времени распространения сигналов. Поскольку это нарушает один из основополагающих принципов метеорной криптографии, то представляется важным оценить влияние невзаимности МРК на возможность ее реализации. Исследование всех затронутых выше вопросов возможно с помощью имитационного моделирования МРК.

2. Имитационная модель метеорного радиоканала

Моделирование метеорного радиоканала произведено согласно методике, изложенной в работах [10, 11]. Структура данной имитационной модели представлена на рис. 2. Важной ее особенностью является использование строгого решения задачи дифракции наклонно падающих радиоволн на метеорном следе, полученном в [12]. Блок электродинамических расчетов позволяет моделировать амплитудно-фазовые характеристики рассеянных на метеорном следе сигналов с учетом воздействия эффекта Фарадея в слоях D и E ионосферы, а также при использовании антенн эллиптической поляризации [13]. Расчеты характеристик сигналов производятся как для прямого, так и для обратного направлений передачи. Ввиду громоздкости расчетных соотношений приводить их здесь нецелесообразно.

В монографии Плеухова [14] представлена систематизация основных причин фазовой невзаимности (ФН) и нестабильности МРК, среди которых особо выделены: эффект Фарадея в ионосфере, многоцентровое рассеяние радиоволн на метеорном следе и смещение отражающей точки метеорного следа ионосферными ветрами. Методика моделирования эффекта Фарадея при метеорном распространении

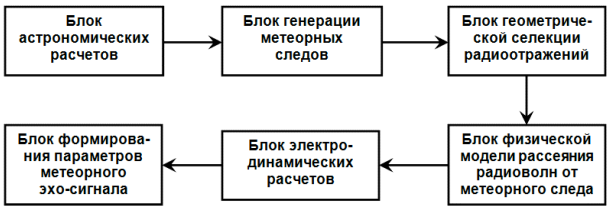
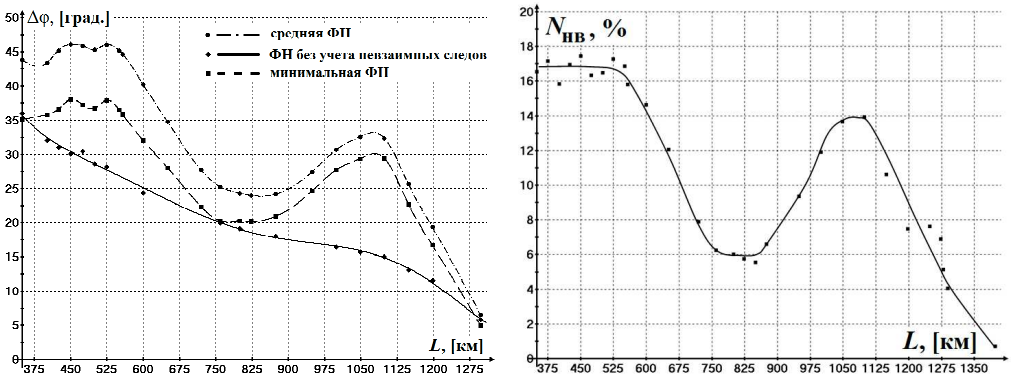


Рис. 2. Блок-схема имитационной модели МРК



а) *б*)

Рис. 3. *а*) ФН для радиолиний различной длины; *б*) доля невзаимных следов

изложена в работе [15]. Имитационное моделирование многоцентрового рассеяния от метеорных следов описано в [16], а учет ветровой нестабильности был осуществлен в [17]. Результаты указанных работ позволяют создать имитационную модель для исследования комплексных закономерностей возникновения фазовой невзаимности МРК и ее количественной оценки.

3. Результаты имитационного моделирования фазовой невзаимности МРК

Для исследования ФН был произведен цикл моделирования двусторонней передачи немодулированных сигналов на несущей частоте $f = 50$ МГц на метеорных радиолиниях различной длины L, ориентированных вдоль лежащей на широте г. Казани параллели 55°47′ с.ш. Порог регистрации $U_{\text{пор}}$ был установлен на уровне −185 дБ относительно передаваемой мощности, использованы антенны горизонтальной поляризации. Для анализа результатов моделирования, помимо классических типов метеорных радиоотражений от переуплотненных (ПУ) и недоуплотненных (НУ) следов, в отдельные классы выделены федингующие следы с многоцентровым рассеянием, резонансные следы с эффектами плазменного резонанса и невзаимные следы, средняя фазовая невзаимность за время регистрации которых превосходит условную границу 90°. Метеорные следы, не относимые к федингующим, резонансным или невзаимным, будем называть «типичными».

Результаты наблюдения средней за продолжительность регистрации метеорного радиоэха фазовой невзаимности $\Delta\phi$ представлены на рис. 3, *а*. Пунктирной кривой изображена зависимость для минимальной в течение радиоэха невзаимности. Отличие ее от средней ФН составляет 3°–8°. Сплошной кривой отображена

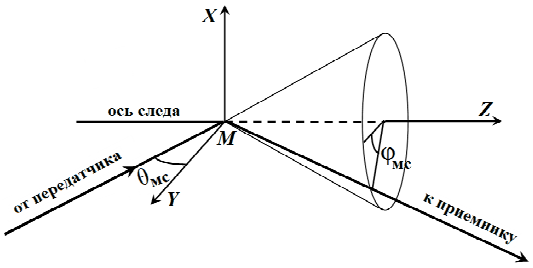


Рис. 4. Геометрия рассеяния на метеорном следе

зависимость средней ФН для выборки, не содержащей следы невзаимного типа. Ее сопоставление с графиком доли невзаимных следов на рис. 3, *б* отчетливо проявляет, что именно невзаимные следы ответственны за возникновение двух пиков, наблюдающихся для длин 500 и 1100 км соответственно.

Вопреки ожиданиям следы резонансного и федингующего типов проявили наименьшую ФН. Доля невзаимных следов у двух этих классов составляет менее 1%, что объясняется слабостью эффекта Фарадея (в среднем всего 10°–15°) на высотах их образования (88–90 км). Такие следы также имеют высокую концентрацию свободных электронов. В особенности это относится к долгоживущим федингующим следам, более 80% которых были классифицированы как ПУ. Падение фазовой невзаимности с возрастанием электронной плотности следа следует непосредственно из решения строгой задачи дифракции [12]. Моделирование показало, что путем повышения порога регистрации следов $U_{\text{пор}}$ можно увеличить долю ПУ, однако это не приводит к значительному падению ФН. Например, повышение порога регистрации на трассе Москва–Казань (длина $L = 720$ км) в 4 раза увеличило долю ПУ с 16% до 26%, при этом ФН упала в среднем всего на 3°. Это заставляет искать иные причины ее возникновения.

С помощью моделирования было также установлено, что наибольшая ФН наблюдается на коротких радиолиниях (менее 500 км). Более 15% регистрируемых на них следов являются невзаимными. С увеличением длины L до величины порядка 830 км происходит падение ФН. Возникновение второго максимума ФН связывается со смещением метеорных следов в область больших высот и резким ростом эффекта Фарадея, который на трассах длиной 875 км у невзаимных следов достигает 200° и более. Показательно и то, что порядка 90% невзаимных следов составляют НУ. Однако дальнейший анализ показал, что главным фактором возникновения невзаимных следов являются ракурсные соотношения между углом падения радиоволны на след $\theta_{\text{мс}}$ и азимутальным углом ее рассеяния $\phi_{\text{мс}}$ (см. рис. 4).

Выявлено, что определяющее значение имеет азимутальный угол рассеяния $\phi_{\text{мс}}$, который является функцией длины радиолинии L. На рис. 5 представлена зависимость среднего значения угла рассеяния $\phi_{\text{мс}}$ от длины радиолинии L для типичных (сплошная линия) и невзаимных (пунктирная линия) следов. Сравнение сплошных кривых на рис. 5 и 3, *а* показывает, что именно увеличение $\phi_{\text{мс}}$ приводит к падению величины ФН. Это является прямым следствием строгого решения задачи дифракции на метеорном следе, анализ которого показывает, что минимум ФН следует ожидать в диапазоне $\phi_{\text{мс}} \in [120^\circ, 160^\circ]$, а в диапазоне $\phi_{\text{мс}} \in [20^\circ, 110^\circ]$, наоборот, достаточно высокую ФН. Последнее подтверждается диаграммами совместного распределения угла падения $\theta_{\text{мс}}$ (по вертикали) и угла рассеяния $\phi_{\text{мс}}$ (по горизонтали), представленными на рис. 6, *а*–*в*. Диаграммы на рис. 6, *а* (невзаимные следы) и рис. 6, *б* (типичные следы) построены для радиолинии длиной 475 км.

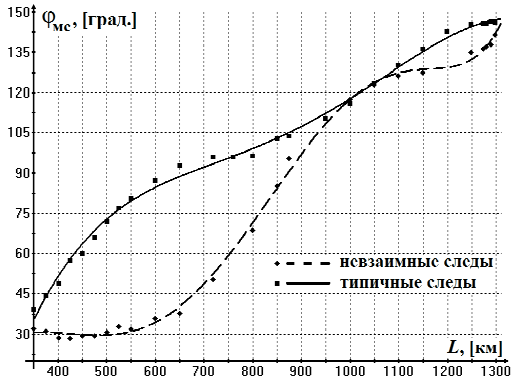


Рис. 5. Азимутальный угол рассеяния для радиолиний различной длины

Из рис. 6, *б* видно, что типичные следы группируются либо в области малых углов $\theta_{\text{мс}}$ и $\phi_{\text{мс}}$, где наблюдается высокая ФН, либо в дугообразной области для достаточно больших значений углов, где ФН, напротив, мала. Снижение средней ФН при увеличении длины радиолинии L связано с падением населенности области с малыми значения углов $\theta_{\text{мс}}$ и $\phi_{\text{мс}}$ и соответственным ростом населенности дугообразной области. Так, на диаграмме рис. 6, *в*, построенной для типичных следов при $L = 1200$ км, мы уже наблюдаем группирование исключительно в дугообразной области. Сравнение рис. 6, *а* и *б* показывает, что невзаимные следы возникают в случаях, когда $\theta_{\text{мс}} \sim \phi_{\text{мс}}$. Напротив, типичные следы «предпочитают» случаи, когда углы падения и рассеяния сильно отличаются по величине друг от друга.

Моделирование также продемонстрировало падение ФН с повышением несущей частоты f. Такое поведение ФН объясняется тем, что суммарный поворот плоскости поляризации радиоволны, приобретаемый ею вследствие эффекта Фарадея как в магнитоактивной плазме ионосферы, так и в магнитоактивной плазме собственно метеорного следа, уменьшается по закону $(1/f)^2$ [15]. Таким образом, с повышением частоты f среда распространения радиоволн приближается по своим свойствам к изотропным средам, что и приводит к ослаблению эффектов невзаимности. Например, повышение частоты на радиолинии Москва–Казань на 10 МГц приводит к падению ФН примерно на 3-4°. Однако повышение частоты существенно ослабляет энергетику радиолинии и количество наблюдаемых метеоров, так как мощность метеорного радиоэха пропорциональна $(1/f)^3$. Другим препятствием к повышению частоты служит необходимость пропорционального повышения и точности синхронизации пунктов связи, что может являться трудноосуществимым.

4. Оценка средней скорости генерации ключевой последовательности

В рамках метеорной криптографии случайные биты, формируемые как результат измерения параметра сигнала X, предлагается использовать в качестве ключа шифрования информации. В качестве X рассмотрим две характеристики регистрируемого сигнала: его фазу ϕ и время распространения от передатчика к приемнику τ. Величина R [бит/с] средней скорости генерации ключевой последовательности на основе значений случайной величины X может быть оценена по формуле

$$R = H(X) \cdot F, \tag{1}$$

где $H(X)$ – энтропия величины X, F – интенсивность снятия ее измерений. В случае метеорного канала величина F ограничена сверху наблюдаемой численностью метеоров $N_{\text{м}}$, испытывающей сложные суточно-сезонные вариации. Типичные ее

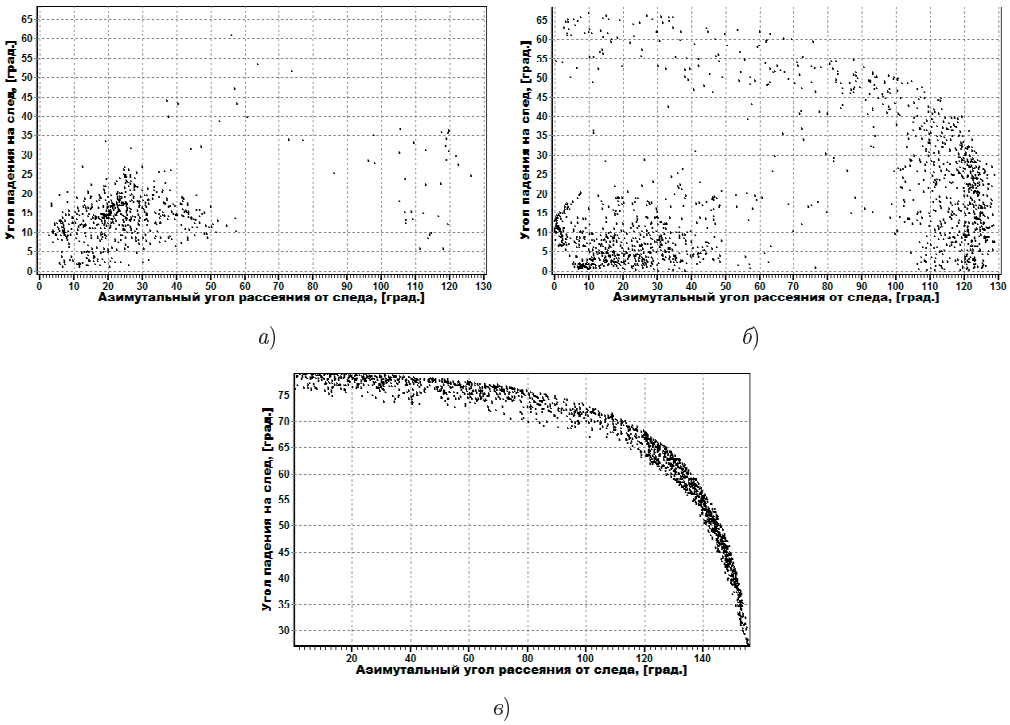


Рис. 6. Диаграммы совместного распределения угла падения и угла рассеяния радиоволны: *а*) для типичных следов при $L = 475$ км; *б*) для невзаимных следов при $L = 475$ км; *в*) для типичных следов при $L = 1200$ км

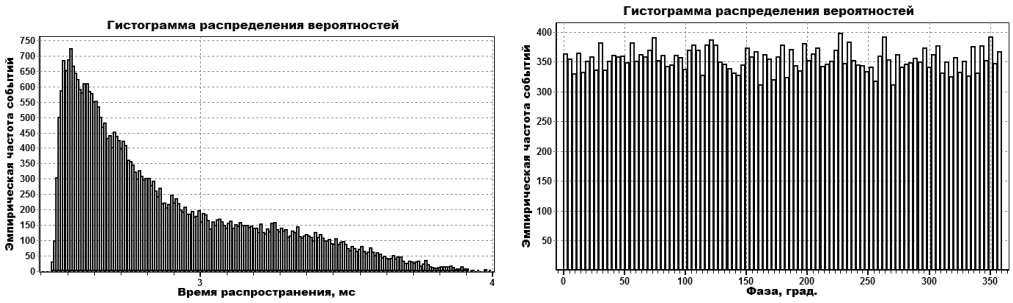
значения лежат в пределах от 50 до 350 метеоров в час. Оценку величин $H(\phi)$ и $H(\tau)$ можно произвести при помощи имитационного моделирования МРК и анализа модельных гистограмм.

На рис. 7, *а*, *б* приведен характерный вид модельных гистограмм распределения времени распространения τ (рис. 7, *а*) и фазы ϕ (рис. 7, *б*), полученных при моделировании радиолинии Москва–Казань ($L = 720$ км). Отсчеты фазы были выбраны на двух сторонах в моменты с наименьшей ФН. Энтропия наблюдаемых величин зависит от разрешающей способности аппаратуры $\delta\tau$ по времени, которая ограничивается погрешностью $\delta\tau_c$ сведения шкал времени пунктов связи A и B и фазовой невзаимностью МРК $\delta\tau_{\text{фн}}$. Суммарную погрешность оценим величиной $\delta\tau = \sqrt{(\delta\tau_c)^2 + (\delta\tau_{\text{фн}})^2}$. Отталкиваясь от результатов опытных испытаний фазовой аппаратуры синхронизации [8], примем, что $\delta\tau_c = 1$ нс.

По результатам моделирования 5000 метеорных регистраций доля невзаимных следов составила около 8%, а усредненная по оставшимся 92% невзаимность $\Delta\phi$ – порядка 20°. В этом случае ошибка невзаимности для частоты 50 МГц составляет 1.1 нс и сопоставима с погрешностью синхронизации $\delta\tau_c$, что доказывает необходимость учета невзаимности МРК. Суммарная погрешность $\delta\tau$ при этом составит 1.5 нс, что эквивалентно погрешности $\delta\phi = 27°$ по фазе несущей.

Моделирование показывает, что разброс τ для радиолинии Москва–Казань составляет от 2500 до 6200 мкс. С учетом погрешности $\delta\tau$ оценка энтропии $\widehat{H}(\tau)$ дает величину 18 бит. Оценка энтропия фазы ϕ получена в предположении равномерности ее распределения (см. рис. 7, *б*) и дает значение $\widehat{H}(\varphi) = 2.7$ бит.

Примем, что наблюдаемая численность метеоров составляет $N_{\text{м}} = 100$ ед./ч, и учтем, что порядка 8% из них подлежат отбраковке по невзаимности. Тогда имеем



а) *б*)

Рис. 7. *а*) модельное распределение времени метеорного распространения τ; *б*) модельное распределение фазы регистрируемых сигналов ϕ

следующие оценки для скорости генерации ключевой последовательности:

$$\begin{cases} R_\tau = H(\tau) \cdot F = 18\ [\text{бит/изм.}] \cdot 92\ [\text{изм./ч}] = 1652\ [\text{бит/ч}] \approx 0.46\ [\text{бит/с}], \\ R_\varphi = H(\varphi) \cdot F = 2.7\ [\text{бит/изм.}] \cdot 92\ [\text{изм./ч}] = 252\ [\text{бит/ч}] \approx 0.07\ [\text{бит/с}]. \end{cases} \quad (1)$$

Таким образом, при одинаковых точностных характеристиках измерительной аппаратуры генерация ключевой последовательности по регистрациям фазы происходит значительно медленнее по сравнению с генерацией ключа по измерениям времени τ. Однако заметим, что сам процесс измерения времени распространения τ на практике требует применения значительно более сложных методик и аппаратуры, чем в случае измерений фазы несущей.

5. Выводы

Показано, что физические свойства метеорного радиоканала могут быть использованы для генерации и распределения ключей симметричного шифрования. Описана методика оценки средней скорости такой генерации. С помощью имитационного моделирования произведены численные оценки фазовой невзаимности метеорного радиоканала для радиолиний различной длины. Показано, что невзаимность падает с повышением несущей частоты и порога регистрации сигналов, а доля метеорных следов с высокой невзаимностью в среднем не превосходит 15–20%. Установлено, что основной причиной возникновения фазовой невзаимности служат соотношения между углами падения и рассеяния радиоволны от метеорного следа. Это обстоятельство объясняет снижение средней величины невзаимности с увеличением длины радиолинии. Оценки показали, что средняя скорость генерации ключевой последовательности составляет примерно 0.1 и 0.5 бит/с при наблюдении за фазой несущей и временем распространения сигналов соответственно. Полученные оценки могут рассматриваться в качестве предельно достижимых значений скорости передачи секретного ключа симметричного шифрования посредством метеорного радиоканала с дальностью действия до 2000 км.

Summary

A.I. Sulimov, A.V. Karpov, O.N. Sherstyukov, V.V. Sidorov, R.G. Khuzyashev. Simulation of Synchronous Generation of Cryptographic Keys in a Meteor Radio Channel.

An evaluation of the generation rate of a symmetric encryption key is performed for the case when a meteor radio channel is used for the symmetric encryption key distribution purposes.

A general method for the generation of a key sequence and a method for the evaluation of its rate are presented. The basic instrumental and physical factors that limit the key generation rate value are discussed. The main regularities and causes of phase non-reciprocity in a meteor radio channel are studied based on a rigorous solution of the radio wave diffraction problems and computer simulation of meteor radio links of different lengths.

Key words: symmetric encryption key, distribution of cryptographic keys, meteor radio channel, diffraction of radio waves, non-reciprocity, non-stability, simulation model, entropy, data rate.

Литература

1. *Смарт Н.* Криптография. – М.: Техносфера, 2005. – 528 с.
2. *Шеннон К.*. Работы по теории информации и кибернетике. – М.: Изд-во иностр. лит., 1963. – 833 с.
3. *Сидоров В.В., Карпов А.В., Сулимов А.И.* Метеорная генерация секретных ключей шифрования для защиты открытых каналов связи // Информ. технологии и вычисл. системы. – 2008. – № 3. – С. 45–54.
4. Пат. 2265957 Российская Федерация. Способ защиты информации в метеорном радиоканале путем шифрования случайным природным процессом / А.В. Карпов, В.В. Сидоров. – № 2004105658/09, заявл. 25.02.2004, опубл. 10.12.2005, Бюл. № 34. – 7 с.
5. Пат. 2370898 Российская Федерация. Способ защиты информации / В.В. Сидоров, А.В. Карпов, А.И. Сулимов. – № 2007134624/09, заявл. 05.09.2007, опубл. 20.10.2009, Бюл. № 29. – 11 с.
6. *Курганов А.Р., Сидоров В.В., Овчинников В.В., Плеухов А.Н., Хузяшев Р.Г.* Экспериментальные исследования фазовой нестабильности и относительной фазовой невзаимности при метеорном и Es распространении радиоволн // Метеорное распространение радиоволн. – 1981. – Вып. 17. – С. 30–39.
7. *Базлов А.Е. Казакова Т.В., Курганов А.Р., Мерзакреев Р.Р., Сидоров В.В., Хузяшев Р.Г., Эпиктетов Л.А.* Экспериментальные исследования невзаимности метеорного радиоканала // Изв. вузов. Радиофизика. – 1992. – Т. 35, № 1. – С. 94–96.
8. *Сидоров В.В., Мерзакреев Р.Р., Эпиктетов Л.А., Логашин А.В., Базлов А.Е.* Аппаратура метеорной синхронизации и связи // 5 Рос. симпозиум «Метрология времени и пространства»: Тр. МВП'94. – Менделеево, 1994. – С. 405–410.
9. *Корнеев В.А., Сидоров В.В., Эпиктетов Л.А.* О возможности защиты информации на основе наносекундной синхронизации шкал времени по метеорным радиоотражениям // Информ. процессы. Электрон. журн. – 2008. – Т. 8, № 1. – С. 10–23. – URL: http://www.jip.ru/2008/10-23-2008.pdf, свободный.
10. *Карпов А.В., Сидоров В.В.* Расчет основных параметров метеорного распространения радиоволн методом статистических испытаний для метеорных радиотрасс произвольной длины // Метеорное распространение радиоволн. – 1980. – Вып. 15. – С. 52–59.
11. *Карпов А.В.* Компьютерная модель метеорного радиоканала // Изв. вузов. Радиофизика. – 1995. – Т. 38, № 12. – С. 1177–1186.
12. *Хузяшев Р.Г.* Расчет амплитудно-фазовых характеристик сигнала при наклонном рассеянии на метеорном следе // Изв. вузов. Радиофизика. – 1984. – Т. 27, № 9. – С. 1110–1113.
13. *Казакова Т.В., Хузяшев Р.Г.* Алгоритм использования табличных результатов строгого решения задачи дифракции волн на метеорном следе в модели метеорного радиоканала // Метеорное распространение радиоволн. – Казань: Изд-во Казан. ун-та, 1991. – Вып. 22. – С. 19–25.

14. *Плеухов А.Н.* КВ канал радиосвязи на частотах выше максимально применимой частоты. – Казань: Изд-во Казан. ун-та, 2000. – 328 с.

15. *Карпов А.В.* Исследование влияния некоторых физических факторов на численность метеорных радиоотражений на длинных трассах // Метеорное распространение радиоволн. – Казань: Изд-во Казан. ун-та, 1981. – Вып. 17. – С. 24–29.

16. *Курганов А.Р., Сидоров В.В.* Моделирование многоцентровости метеорных следов и ограничения полосы пропускания метеорного канала // Метеорное распространение радиоволн. – Казань: Изд-во Казан. ун-та, 1991. – Вып. 22. – С. 55–65.

17. *Карпов А.В., Сидоров В.В.* Моделирование ветровой фазовой нестабильности метеорного радиоканала // Метеорное распространение радиоволн. – Казань: Изд-во Казан. ун-та, 1980. – Вып. 16. – С. 48–51.

Поступила в редакцию
18.10.11

Сулимов Амир Ильдарович – ассистент кафедры радиофизики Казанского (Приволжского) федерального университета.
E-mail: *Amir.Sulimov@ksu.ru*

Карпов Аркадий Васильевич – доктор физико-математических наук, профессор кафедры радиофизики Казанского (Приволжского) федерального университета.
E-mail: *Arkadi.Karpov@ksu.ru*

Шерстюков Олег Николаевич – доктор физико-математических наук, заведующий кафедрой радиофизики Казанского (Приволжского) федерального университета.
E-mail: *Oleg.Sherstyukov@ksu.ru*

Сидоров Владимир Васильевич – доктор физико-математических наук, профессор кафедры радиофизики Казанского (Приволжского) федерального университета.
E-mail: *Vladimir.Sidorov@ksu.ru*

Хузяшев Рустэм Газизович – кандидат физико-математических наук, доцент кафедры «Электроэнергетические системы и сети» Казанского государственного энергетического университета.
E-mail: *142892@mail.ru*